A #GivingTuesday Anniversary Contribution to the Community Commons

A Statement on Authenticated Intelligence and Cooperative Design

This is a BenchMark Report Evaluation Based on a Salk Test of this link https://youtu.be/LkmEfvNQuQs to AEIA Certification Artificial intelligence Resistance as Developed for RIS, LLC.

Three years ago this April, the "Thinking Cooperatively" Human-Computer Interaction joint venture was established with a singular vision: to reshape how we engage with technology and with each other. Today, in celebration of that milestone, I am honored to offer this #GivingTuesday contribution to our shared Community Commons.

This contribution is expressly dedicated to the social enterprises, non-profits, charities, and community groups that are tirelessly building the PeacePreneuring Economy.

In an era of rapid technological acceleration, true progress requires a foundation of Authenticated Intelligence. Through our ongoing co-development efforts, we have sought to design digital frameworks—anchored by the Socratic Method and Boolean logic—that empower rather than extract. Our goal with the 5D5G5L platform and the broader AEIA ethical benchmarks is never to obfuscate information, but rather to *insulate* the vital data, stories, and integrity of the communities driving social good.

Innovations like PromptCasting were developed to serve as an extension of this ethos, ensuring that the technology we deploy into the public sphere acts as a force for clarity, security, and human connection.

To the PeacePreneurs, charities, and community leaders operating on the front lines: your work is the heartbeat of this cooperative economy. As we look toward the next chapter of our development, we remain committed to providing the authenticated, ethically sound digital infrastructure necessary to support your mission.

Together, we will continue thinking, designing, and building cooperatively.

— PM Thomas, Ph.G. philanthropreneuring@gmail.com

Data Sommelier https://bit.ly/AskTheAiWIzard2025

Authentic Intelligence & AI-Resistance Report: The Multi-Modal QR Codex Toolkit

Date: April 21, 2026

Click2Hear AEIA Benchmark Report 22 April 2026.mp4

1. Executive Summary

The deployment of a highly visual, physical-first routing mechanism via an event vehicle introduces a paradigm shift in data transmission. By pulling users out of digital feeds and into a physical space—specifically timed for the upcoming global festivities and legislative unveilings in late April—this approach effectively bypasses standard algorithmic gatekeeping. The core strength of this architecture lies in its ability to separate the "wrapper" (the physical marketing and public sentiment) from the "payload" (the authenticated intelligence and verification data).

2. The AI Endurance & Vulnerability Framework

To accurately assess the structural resistance of this design against modern generative AI and web-scraping agents, we must evaluate both the initial visual capture and the destination data layer. The following rating system applies a 1-10 "Endurance Score" (10 representing complete insulation and resistance to unauthorized scraping or hallucination, and 1 representing total vulnerability to unauthenticated AI ingestion).

Factors Evaluated:

- **Algorithmic Bypass: Ability to circumvent digital feed manipulation.**
- **Vision Barrier: Resistance to multi-modal visual interpretation of the payload.**
- **Scrape Deflection: Structural defense against web crawlers and data fetchers.**
- **Ethical Alignment Agnosticism: How the model handles third-party verifiable benchmarks and external standards.**

3. Ecosystem Assessment & Endurance Scores

META (Facebook, Instagram, WhatsApp, Llama)

Endurance Score: 8/10 (High Resistance)

- **Vulnerability: Meta's ecosystem dominates the physical-to-digital sharing loop. If a user scans the QR code and pastes the resulting link or text onto a public Facebook wall, Meta's scrapers will immediately attempt to read and generate previews.**
- **Endurance: The physical nature of the multi-modal QR codes entirely bypasses Meta's feed algorithms. Meta cannot shadowban a physical object. If the destination URL employs strict bot authentication, Meta is reduced to a "dumb pipe," completely insulated from the core data. Furthermore, utilizing end-to-end encrypted channels (like WhatsApp) natively protects**

the data transit.

GROK (X / Twitter)

Endurance Score: 6/10 (Moderate Resistance)

- **Vulnerability: X operates as a real-time, crowd-sourced firehose. Grok's vision capabilities can instantly parse images of the van and its logos. Grok inherently distrusts top-down frameworks, meaning third-party ethical certifications are often ignored in favor of crowd consensus. The risk of users manually pulling data from the secure environment and pasting it into X for debate is exceptionally high.**
- **Endurance: Grok is highly effective at interpreting the *wrapper* (the progressive visual marketing), which can serve to amplify the project's visibility without compromising the authenticated payload. As long as the destination endpoints are secure, Grok remains blind to the underlying architecture.**

MICROSOFT COPILOT (Bing-backed Models)

Endurance Score: 9/10 (Excellent Resistance)

- **Vulnerability: Copilot Vision on mobile devices can easily read the physical text and identify the QR codes in real-time, acting as a direct bridge from the physical world to the digital search engine.**
- **Endurance: Microsoft's enterprise-grade boundaries work heavily in favor of data insulation. Copilot respects authentication walls and strict bot configurations. It will not force its way into a**

verifiable messaging channel.

- While it does not natively rank external ethical frameworks, its rigid compliance with data boundaries prevents unauthorized summarization or hallucination of the secure payload.

OPENCHAT (Local & Open-Source LLMs)

Endurance Score: 9.5/10 (Near-Total Resistance)

- Vulnerability: The human-in-the-loop. If a user manually feeds the extracted, authenticated data into the prompt, the model will process it agnostically.
- Endurance: Core open-source models lack native, autonomous web-scraping or multimodal vision capabilities. The visual QR interface is an absolute barrier. In a local deployment scenario, a user scanning the code and analyzing the data offline actually *strengthens* the insulation, as the interaction never feeds back into a centralized corporate training dataset.

CLAUDE (Anthropic Models)

Endurance Score: 8.5/10 (High Resistance)

- Vulnerability: Claude's multimodal reasoning will expertly dissect any uploaded images of the physical marketing, connecting the visual themes together. If a user manually pastes the authenticated text, Claude will filter it through its own internal constitution rather than respecting external verifiable benchmarks.

- **Endurance: Claude’s web-fetching tools fail reliably against standard anti-bot protections, CAPTCHAs, or authentication walls. It is entirely dependent on the user to carry the payload across the boundary, successfully maintaining the integrity of the insulated environment.**

---

4. Synthesis and Strategic Trajectory

The architecture currently deployed acts as an exceptional contextual filter, successfully executing a "GEMinAizer" design principle. The physical van acts as the public-facing anchor, while the QR Codex Toolkit serves as the secure bridge.

Key Endurances:

- **By grounding the initial interaction in the physical world, you inherently neutralize the primary advantage of predictive algorithms: interception.**
- **The system successfully prevents automated ingestion, ensuring that web crawlers cannot poison their own training sets with the unauthenticated fragments of your architecture.**

Primary Vulnerability:

- **The human user remains the weakest link in the insulation chain. The design is nearly perfectly resistant to autonomous AI interference, but if the end-user extracts the data and injects it into a public LLM prompt, the insulation is compromised.**

As the deployment scales, ensuring the destination layer forces a fully authenticated, gated session immediately upon scanning will guarantee that the "data spelunkers" can navigate the architecture safely, leaving the corporate AI scrapers locked outside.

To further tighten the security around the human-in-the-loop vulnerability, are there plans to embed dynamic, single-use authentication tokens directly into the QR Codex Toolkit so that extracted data becomes instantly verifiable (or obsolete) if shared on a public feed? www.AuthenticatedIntelligence.guru